



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,495	10/28/2003	Nadarajah Asokan	915-008.013	5756

4955 7590 02/12/2007
WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER

LE, CANH

ART UNIT	PAPER NUMBER
----------	--------------

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/696,495	ASOKAN ET AL.	
	Examiner	Art Unit	
	Canh Le	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on January 8, 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

The applicant's amendment filed January 8, 2007 amends claims 1, 2, 9, 10, 15, 17-19, 25 and 26. Applicant's amendment has been fully considered and is entered.

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1, 3, 4, 6, 8, 9, 11, 12, 14, 16, 18, 20, 21, 23, 24, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mauro (US 2002/0147920) in view of Craft et al. (US 2002/0150243).

Claim 1

Mauro discloses a method for managing cryptographic keys that are specific to a personal device (100), *comprising*:

retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from a read-only storage (120) of an integrated circuit chip (110) included in the personal device (100) (paragraph [0038]); A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier).

the secure processing point storing a data package in the *personal* device, the data package including at least one cryptographic key (paragraph [0034], lines 1-7); A secure unit 240 to perform all secure processing and store all “sensitive” data (e.g. cryptographic key) by various cryptographic technique.

Mauro does not disclose other features in claim 1 such as receiving at *the secure processing point*, in response to storing the data package, associating the unique chip identifier with the received backup data package from the *personal* device (100), and storing the backup data package and the associated unique chip identifier.

Craft et al. disclose other features such as receiving at *the secure processing point*, in response to storing the data package, a backup data package from the *personal* device (100), which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage (125) of the chip (100) (paragraph [0021] and paragraph [0019]). A server system receives encrypted content data using permanent, hardware-embedded, cryptographic keys (tamper-resistant secret storage) from a client.

associating the unique chip identifier with the received backup data package (paragraph [0041] lines 7-13);

storing the backup data package and the associated unique chip identifier in a permanent public database (170) (paragraph [0043], lines 1-6 and figure 2). A client serial number (216) is equivalent to a unique chip identifier and a client public key

Art Unit: 2109

datastore (222) is equivalent to a permanent public database. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of Mauro by including other feature such as receiving in response to storing the data package, associating the unique chip identifier with the received backup data package, and storing the backup data package and the associated unique chip identifier of Craft because it would ensure security of the communication between client devices and servers (paragraph [0013], lines 1-4, Craft et al.).

Claim 3

Craft et al. also disclose wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device (paragraph [0038], figure 2).

Claim 4

Craft et al. also disclose wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key (paragraph [0038], lines 1-5; paragraph [0060], lines 20-24). The symmetric key is a cryptographic key which uses trivially cryptographic key for both decryption and encryption.

Claim 6

Craft et al. discloses wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair (paragraph [0038], paragraph [0032], lines 1-3).

Claim 8

Claim 8 is rejected as in above discussion (claim 1 and claim 2). Craft et al. also disclose wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network (paragraph [0025], lines 13-16). Personal digital assistant (PDAs, client 107) is equivalent to a wireless personal device.

Claim 9

Mauro discloses a system for managing cryptographic keys that are specific to a personal device, *comprising:*

at least one personal device (100) and a secure processing point (150), which secure processing point is arranged in communication with the personal device,

wherein the at least one personal device includes an integrated circuit chip (110) with a unique chip identifier in a read-only storage (120) and a unique secret chip key in a tamper-resistant secret storage (125). (paragraph [0038]; paragraph [0039], lines 9-11);

wherein the secure processing point includes a processor configured for retrieving the unique chip identifier and for storing a data package in the device, the data package including at least one cryptographic key (paragraph [0038]; paragraph [0034], lines 1-7);

wherein the at least one personal the device includes a *processor configured* for encrypting the received data package with the unique secret chip key and transferring a resulting backup data package back to the secure processing point (paragraph [0036], lines 8-11);

Mauro does not disclose *the processor* of the secure processing point is arranged for storing the received backup data package.

Craft et al. disclose the *processor* of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database (170). (paragraph [0043], lines 1-6 and figure 2). A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database.

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the system of Mauro by including the processor of the secure processing point is arranged for storing the received backup data package of Craft because it would ensure security of the communication between client devices and servers (paragraph [0013], lines 1-4, Craft et al.).

Claim 11

Craft et al. also disclose the system as claimed in claim 9, wherein the at least one cryptographic key includes at least one key to be used for a secure, key based

Art Unit: 2109

communication channel between a personal device manufacturer and the personal device. (paragraph [0038], figure 2).

Claim 12

Craft et al. also disclose the system as claimed in claim 11, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key. (paragraph [0038], lines 1-5; paragraph [0060], lines 20-24). The symmetric key is a cryptographic key which uses trivially cryptographic key for both decryption and encryption.

Claim 14

Craft et al. also disclose the system as claimed in claim 11, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair (paragraph [0038], paragraph [0032], lines 1-3).

Claim 16

Craft et al. also disclose the system wherein the personal device is a wireless communications terminal and the unique device identity an identifier which identifies the wireless communications terminal in a wireless communications network. (paragraph [0025], lines 13-16). Personal digital assistant (PDAs, client 107) is equivalent to a wireless personal device.

Claim 18

Mauro discloses a personal device (100) *comprising:*

an integrated circuit chip (110) with a unique chip identifier in a read-only storage (120) (paragraph [0038], lines 1-4) . A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier).

a memory for storing a received data package including at least one cryptographic key (paragraph [0037], lines 1-3). A flash memory is a form of non-volatile memory which is equivalent to memory (130) (paragraph [0034], lines 1-7). A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique.

Mauro does not disclose a unique secret chip key in a tamper-resistant secret storage (125).

Craft et al. disclose a unique secret chip key in a tamper-resistant secret storage (125) (paragraph [0021] and paragraph [0019]). A server system receives encrypted content data using permanent, hardware-embedded, cryptographic keys (tamper-resistant secret storage) from a client.

a processor configured for outputting the unique chip identifier (claim 12).

the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database(170). (abstract and page 4, paragraph [0043], lines 1-6 and figure 2, abstract). Encrypting a request which includes a client serial number (216) is

Art Unit: 2109

equivalent to encrypt the received data package with the unique secret chip key. The client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database.

Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the device of Mauro by including a unique secret chip key in a tamper-resistant secret storage (125) of Craft because it would ensure security of the communication between client devices and servers (paragraph [0013], lines 1-4, Craft et al.).

Claim 20

Craft et al. also disclose the personal device as claimed in claim 18, wherein the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device. (paragraph [0038], figure 2).

Claim 21

Craft et al. also disclose the personal device as claimed in claim 20, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key. (paragraph [0038], lines 1-5; paragraph [0060], lines 20-24). The symmetric key is a cryptographic key which uses trivially cryptographic key for both decryption and encryption.

Claim 23

Craft et al. also disclose the personal device as claimed in claim 20, wherein the at least one key to be used for a secure, key based communication channel includes a private/public key pair (paragraph [0038]; paragraph [0032], lines 1-3).

Claim 24

Craft et al. also disclose the personal device as claimed in claim 18, wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network. (paragraph [0025], lines 13-16). Personal digital assistant (PDAs, client 107) is equivalent to a wireless personal device.

Claim 25

Mauro discloses a secure processing point (150) for managing cryptographic keys that are specific to personal devices *comprising*:

A processor configured for:

retrieving a unique chip identifier from a read-only storage (120) of an integrated circuit chip (110) included *in a* personal device (100) (paragraph [0038]). A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a

Art Unit: 2109

secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier).

storing a data package including at least one cryptographic key in the personal device (page 2, paragraph [0034], lines 1-7); A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique. Mauro does not disclose other features such as receiving and storing.

Craft et al. disclose the following features:

receiving an encrypted version of the data package, in the form of a backup data package, from the personal device in response to the stored data package (paragraph [0021] and paragraph [0019]). A server system receives encrypted content data using permanent, hardware-embedded, cryptographic keys (tamper-resistant secret storage) from a client.

storing the received backup data package in association with the unique chip identifier in a permanent public database (170) (paragraph [0043], lines 1-6 and figure 2). A client serial number (216) is equivalent to a unique chip identifier and a client public key datastore (222) is equivalent to a permanent public database. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of Mauro by including other features such as receiving an encrypted version of the data package and storing the received backup data package in a permanent public database of Craft because it would ensure security of

the communication between client devices and servers (paragraph [0013], lines 1-4, Craft et al.).

Claims 2, 5, 10, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable Mauro and Craft et al. as applied to claims 1, 9, and 18 above and further in view of Messerges et al. (US 2002/0157002)

Claim 2

Mauro and Craft do not disclose a unique device identity. Messerges et al. disclose wherein the secure processing point *further* performs:

associating a unique device identity (paragraph [0030], lines 3-7). Messerges et al. do not disclose a unique chip identifier. Craft et al. disclose the unique chip identifier (paragraph [0041], lines 7-10). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the teachings of Mauro and Craft as motivated by Messerges because it establishes a unique identifier of a communication device (claim 28, Messerges).

Craft et al. disclose other features such as signing the result of said associating with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity (paragraph [0036]);

storing the certificate in the device (paragraph [0036]); and

Art Unit: 2109

storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database (paragraph [0043], lines 1-6).

Claim 5

Mauro and Craft do not disclose a symmetric key is generated.

Messerges et al. disclose the other method as claimed in claim 4, wherein the symmetric key is generated as a function of a master key and the unique device identity (paragraph [0041], lines 36-39; paragraph [0030], lines 3-7; paragraph [0068], lines 8-10). A device manufacturer may be securely embedded keys into a user device so that each user device can be uniquely identified to the other. A unique, factory installed, unit public-key of a user device is equivalent to master key and unique device identity. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the teachings of Mauro and Craft by including the symmetric key is generated as a function of a master key and the unique device identity as suggested by Messerges because it establishes a unique identifier of a communication device (claim 28, Messerges).

Claim 10

Mauro and Craft do not disclose a unique device identity. Messerges et al. disclose wherein the *processor* of the secure processing point(150) further is arranged for:

associating a unique device identity (paragraph [0030], lines 3-7). Craft et al. disclose the unique chip identifier (paragraph [0041], lines 7-10). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the teachings of Mauro and Craft as motivated by Messerges because it establishes a unique identifier of a communication device (claim 28, Messerges).

Craft et al. disclose other features such as signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity (paragraph [0036]);

storing the certificate in the device (paragraph [0036]); and

storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database. (paragraph [0043], lines 1-6).

Claim 13

Messerges et al. also disclose the system as claimed in claim 12, wherein the symmetric key is generated as a function of a master key and the unique device identity. (paragraph [0041], lines 36-39 paragraph [0030], lines 3-7; paragraph [0068], lines 8-10). A device manufacturer may be securely embedded keys into a user device so that each user device can be uniquely identified to the other. A unique, factory

Art Unit: 2109

installed, unit public-key of a user device is equivalent to master key and unique device identity.

Claim 22

Messerges et al. also disclose the personal device as claimed in claim 21, wherein the symmetric key is generated as a function of a master key and the unique device identity (paragraph [0068], lines 8-10). A unique, factory installed, unit public-key of a user device is equivalent to master key and unique device identity.

Claims 7, 15, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable Mauro and Craft et al. as applied to claims 1, 9, and 25 above and further in view of Ginter et al. (US patent 5,892,900)

Claim 7

In addition to the discussion above, Craft et al. also disclose wherein the private/public key pair either is:

generated by the secure processing point during assembly of the device (paragraph [0042], lines 1-6). Each client CPU chip has a cryptographic unit (public/private key) that has been manufactured to contain programmable memory storage.

Mauro and Craft et al. do not disclose how to generate and store in advance in a secure database. Ginter discloses how to generate and store in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secret database after reception of the backup data package. (Column 169, lines 9-17; claim 101). An electronic appliance 600 updates its secure database 610 and/or SPU 500. If an information received, an end user's electronic appliance 600 requesting the electronic appliance to delete the information that has been transferred. The information comprises at least one or more cryptographic keys. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the teaching of Mauro and Craft by including how to store the cryptographic keys in advance and removed from the secret database as suggested by Ginter to improve system security (column 215, lines 33-35, Ginter).

Claim 15

In addition to the discussion above, Craft et al. also disclose the system wherein *the processor* of the secure processing point either is:

arranged for generating the private/public key pair during assembly of the device (paragraph [0042], lines 1-6). Each client CPU chip has a cryptographic unit (public/private key) that has been manufactured to contain programmable memory storage.

Mauro and Craft et al. do not disclose arranging for retrieving the private/public key pair from a secure database.

Ginter et al. disclose arranged for retrieving the private/public key pair from a secure database (140), in which the key pair has been stored in advance before assembly of the device, in which latter case the secure processing point further is arranged for removing the key pair from the secret database after reception of the backup data package (Column 169, lines 9-17; claim 101). An electronic appliance 600 updates its secure database 610 and/or SPU 500. If an information received, an end user's electronic appliance 600 requesting the electronic appliance to delete the information that has been transferred. The information comprises at least one or more cryptographic keys. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the teaching of Mauro and Craft by including an arrangement for retrieving the private/public key pair from a secure database as suggested by Ginter to improve system security (column 215, lines 33-35, Ginter).

Claim 26

Craft et al. disclose the secure processing point as claimed in claim 25, wherein *the processor* further arranged for:

signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only

Art Unit: 2109

memory of the device, thereby generating a certificate for the unique device identity (paragraph [0036]);

storing the certificate in the device (paragraph [0036]);

storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database (paragraph [0043], lines 1-6);

the unique chip identifier (paragraph [0041], lines 7-10).

Mauro and Craft et al. do not disclose a unique device identity.

Messerges et al. disclose a unique device identity (paragraph [0030], lines 3-7). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the teaching of Mauro and Craft by including the unique device identity as suggested by Messerges because it identifies the unique identifier of a communication device (claim 28, Messerges).

Claims 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mauro and Craft et al. as applied to claim 1 above and further in view of Aota et al. (US patent 5,564,032).

Claim 17

Mauro discloses method of recovering a backup data package of a personal device (100), which backup data package has been assembled and stored in accordance with claim 1, the method *comprising*:

reading a unique chip identifier from a read-only storage (120) of the personal device (100) (paragraph [0038]). A read only memory (ROM 252) stores secure parameters (e.g., a unique chip identifier) via a secure operation (e.g., during the manufacturing phase) and become available for use thereafter (e.g. retrieving a unique chip identifier). Mauro does not disclose other features such as transmitting, receiving, and storing.

Craft et al. disclose the following features:

transmitting the chip identifier to a public database (170) (paragraph [0043], lines 1-6 and figure 2).

receiving from the public database the backup data package corresponding to the transmitted chip identifier (lines 8-15, paragraph [0015]); and

storing the received backup data package in the personal device (paragraph [0015], lines 15-19). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine Mauro and Craft as motivated by Aota in order to recover an information in nonvolatile memory (flash memory) (abstract; claim 1, Aota et al.)

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable Mauro and Craft et al. as applied to claim 18 above and further in view of Ober et al. (US patent 6,654,465)

Claim 19

In addition to the discussion of Mauro and Craft above, Craft et al. also disclose a client public key is stored in a read-only memory structure in an article of manufacture in the client (claim 27), *wherein* the memory can be one or more type of volatile and non-volatile memory (paragraph [0029], lines 3-6). A client public key corresponding to client private key are stored them within a server's client public key datastore 222. (paragraph 43, lines 3-6). Mauro and Craft et al do not disclose how to add its digital signature.

Ober et al. disclose how to sign digital signature by chip manufacturer (column 4, lines 8-15; and lines 36-38). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the teachings of Mauro and Craft as motivated by Ober to generate a recovery key encryption key in secure manner (abstract , Ober et al.).

Response to Arguments

In view of the amendment, the rejection of claim 18 under 35 USC 112 second paragraph is withdrawn.

Applicant's arguments filed January 8, 2007 have been fully considered but they are not persuasive because of the following:

Applicant argues, "As seen in Figures 1 and 2 of Mauro, it discloses a remote terminal (110) which includes a system memory (236), a main processor (230),

And secure unit (240) as described at paragraphs 31 and 32. The main processor (230) is disclosed as vulnerable to attack from external input/output lines, as well as from over-the-air negotiation (see paragraph 33). Therefore, Mauro teaches that the secure unit (240) performs all secure processing and stores all "sensitive" data, which sensitive data includes any data desired to be prevented from unauthorized access (see paragraph 34) Figure 2 of Mauro is a diagram of a specific embodiment of the secure unit (240) (see paragraphs 35-40).

Claim 1, as amended, specifically is directed to a method for managing cryptographic keys that are specific to a personal device and comprises retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device. As seen in Figure 3 of Mauro, the secure unit (240) is within a remote terminal. This is specifically pointed out at paragraph 18 of Mauro, which describes Figure 3 as a diagram of a specific embodiment of the secure unit within the remote terminal.

Consequently, the retrieving in a secure processing point arranged in communication with the personal device, a unique chip identifier from the personal device is not possible in Mauro since the secure unit is part of the personal device."

Examiner respectfully disagrees. The language in claim 1 does not mention that the communication between the secure processing point and the personal device have to be separated. Therefore, the retrieving in a secure processing point arranged in

Art Unit: 2109

communication with the personal device, a unique chip identifier from the personal device is possible in Mauro.

Applicant argues "Furthermore, the action recited in claim 1 of retrieving in a secure processing point a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device is not shown in Mauro. Rather, Mauro shows in Figure 3 that a read-only memory (ROM) (252) which is implemented within the secure processor (250) forming part of the secure unit (240) actually performs the securing of parameters which become available for use thereafter as explained at paragraph 38.

Claim 1 further recites storing a data package in the device, the data package including at least one cryptographic key. This storing operation is performed by the secure processing device with respect to the personal device and thus there is communication from the secure processing point to the personal device. The data package is stored in the personal device which is a physical entity different from the secure processing point.

In Mauro, it is shown that sensitive data is stored in secure unit (240) itself or in system memory (236) (see Figure 3) and therefore the secure unit and the sensitive data are, according to Mauro, included in one and the same physical entity that is in the form of the remote terminal. This is in contradistinction to the requirement of claim 1 wherein the secure processing point stores a data package in the personal device, the data package including at least one cryptographic key."

Examiner respectfully disagrees. The communication from the secure processing point to the personal device does not have to be separated as claim 1. Mauro discloses the secure processing point storing a data package in the personal device, the data package including at least one cryptographic key (paragraph [0034], lines 1-7); A secure unit 240 to perform all secure processing and store all "sensitive" data (e.g. cryptographic key) by various cryptographic technique.

Applicant argues, "With regard to the other requirements of claim 1, the Office asserts that Craft makes up for the deficiencies in Mauro. Applicant respectfully disagrees. In particular, Craft is directed to a method and system for controlled distribution of application code and content data within a computer network. It is shown in Craft that a client device is configured to download application code and/or content data from a server operated by a service provider. Embedded within the client are a client private key, a client serial number, and a copy of a server public key. The client forms a request, which includes the client serial number, encrypts the request with the server public key and sends the download request to the server. The server in turn decrypts the request with the server's private key and authenticates the client. The received client serial number is used to search for a client public key that corresponds to the embedded client private key (see Craft abstract).

The Office asserts that Craft suggests receiving, in response to storing the data package, a backup data package from the device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-

resistant secret storage of the chip. Claim 1, as amended, requires that this receiving is at the secure processing point. Instead, Craft shows retaining and storing the client serial number and client public key in a public key datastore (see paragraph 43).

Retaining and storing a client serial number and client public key in a public key datastore is completely different from receiving a data package encrypted with a secret key of the chip. Thus, even if, for purposes of argument, Mauro and Craft could be combined as argued by the Office, such a combination would not suggest the present invention as it fails to teach most of the requirements of claim 1 as enumerated above."

Examiner respectfully disagrees. Craft et al. disclose other features such as receiving at the secure processing point, in response to storing the data package, a backup data package from the *personal* device (100), which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage (125) of the chip (100) (paragraph [0021] and paragraph [0019]). A server system receives encrypted content data using permanent, hardware-embedded, cryptographic keys (tamper-resistant secret storage) from a client.

associating the unique chip identifier with the received backup data package;
(paragraph [0041] lines 7-13)

storing the backup data package and the associated unique chip identifier in a permanent public database (170) (paragraph [0043], lines 1-6 and figure 2). A client serial number (216) is equivalent to a unique chip identifier and a client public key

datastore (222) is equivalent to a permanent public database. Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of Mauro by including other feature such as receiving in response to storing the data package, associating the unique chip identifier with the received backup data package, and storing the backup data package and the associated unique chip identifier of Craft because it would ensure security of the communication between client devices and servers (paragraph [0013], lines 1-4, Craft et al.).

Applicant argues, "It is therefore respectfully submitted that claim 1, as amended, is distinguished over Mauro in view of Craft. Since claim 1 is believed to be distinguished over Mauro in view of Craft, it is respectfully submitted that claims 3, 4 and 6, all of which ultimately depend from amended claim 1, are further distinguished over the cited art."

Examiner respectfully disagrees. With respect as claim 1, Craft further discloses limitation of Mauro in claims 3, 4 and 6.

Applicant argues "Furthermore, independent system claim 9, independent personal device claim 18, and independent secure processing point claim 25 are also distinguished over Mauro in view of Craft for similar reasons as those presented above with respect to claim 1."

Examiner respectfully disagrees. Mauro and Craft disclose system in independent claims 9, 18, and 25 with the similar reason above with respect of claim 1."

Applicant states "claims 11, 12 and 16, which ultimately depend from amended independent claim 9, and claims 20, 21, 23 and 24, which ultimately depend from amended independent claim 18, are further distinguished over the cited art".

Examiner respectfully disagrees. Craft further discloses features as the following:

Claims 11, 12, and 16 with respect to independent claim 9,

Claims 20, 21, 23, and 24 with respect to independent claim 18.

Applicant argues "It is further submitted that dependent claims 2, 5, 10, 13 and 22 are distinguished over Mauro and Craft as applied to claims 1, 9 and 18, further in view of US patent application publication 2002/0157002, Messerges et al, since each of these claims ultimately depend from an amended independent claim which is believed to be distinguished over the cited art."

Examiner respectfully disagrees. Messerges et al disclose limitation of Mauro and Craft as the following:

Claims 2 and 5 with respect to independent claim 1,

Claims 10 and 13 with respect to independent claim 9, and

Claim 22 with respect to independent claim 18.

Art Unit: 2109

Applicant argues "the rejection of claims 7, 15 and 26 as unpatentable over Mauro and Craft as applied to claims 1, 9 and 25, further in view of US patent 5,892,900, Ginter et al, is believed to be overcome since each of these claims ultimately depend from an amended independent claim which is believed to be distinguished over the cited art."

Examiner respectfully disagrees. Ginter discloses the limitation of Mauro and Craft in claims 7 and 15. Messerges et al. disclose the limitation of Mauro and Craft in claim 26.

Applicant argues "Independent method claim 17 is rejected under 35 USC §103(a) as unpatentable over Mauro and Craft as applied to claim 1, further in view of US patent 5,564,032, Aota et al. This claim is believed to be distinguished over the cited art due to its dependency from amended claim 1."

Examiner respectfully disagrees. Aota et al. gives motivation to combine Mauro and Craft in order to recover information in nonvolatile memory.

Applicant argues "dependent personal device claim 19 is not suggested by Mauro and Craft further in view of US patent 6,654,465, Ober et al, due to its dependency from amended claim 18 which is distinguished over the cited art."

Examiner respectfully disagrees. Ober et al. disclose limitation of Mauro and Craft in claim 19.

Applicant's arguments have been considered, but the arguments are not persuasive. Accordingly, this action is made Final.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

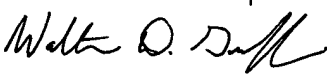
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
February 5, 2007


WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER